Le *fingerprinting*, plus pernicieux que les cookies

La prise d'empreinte numérique est plus persistante que le cookie, qui peut s'effacer ou se refuser.

Par **Thomas Bernard**

La technique permet d'identifier un appareil selon plusieurs paramètres matériels et logiciels. Désormais autorisée par Google, elle interroge sur la confidentialité en ligne.

Il ne s'agit pas d'une scène de crime, mais les empreintes traînent pourtant partout. Celles-ci sont numériques, invisibles, indélébiles. Chaque internaute en dépose des fragments en permanence, dès qu'il surfe sur le Web: la configuration de son navigateur Internet est connue, le type d'appareil également, tout comme la langue qu'il utilise ou encore son fuseau horaire, formant ainsi une somme de paramètres.

Mis bout à bout, chaque petit morceau d'information permet d'isoler progressivement un internaute au sein d'une masse de visiteurs. Il faut en croiser un certain nombre pour dresser une empreinte unique, appartenant à un individu.

Cette technique dite du *fingerprinting*, soit la prise d'empreintes numériques, permet un suivi en ligne ou le ciblage publicitaire d'un internaute, sans recourir à des cookies traditionnels. Ces derniers peuvent s'effacer ou se refuser, alors que l'empreinte, plus persistante, colle à l'utilisateur. Si la technique n'est pas neuve, son intérêt s'est réaffirmé avec la mise en œuvre du Règlement général sur la protection des données (RGPD) européen et le refus grandissant des cookies.

Moins informative, mais plus efficace

Contrairement à ces derniers qui conservent des informations plus détaillées, éventuellement transmises à des tiers, l'empreinte numérique est basique. «Pour faire court, les cookies permettent d'enregistrer tout ce qui est consulté en ligne. Le *fingerprinting*, c'est tout l'environnement matériel et logiciel qui permet la consultation», vulgarise Axel Legay, expert en cybersécurité chez Nexova, entreprise spécialisée dans la cybersécurité.

Ce procédé est donc moins utile pour savoir ce qui est fait, mais plus pérenne pour identifier un internaute. Combien de services l'exploitent véritablement? Difficile, voire impossible à dire. Mais ses avantages sont clairs, notamment pour combattre la fraude ou le détournement

ILLUSTRATIONS RÉALISÉES PAR UNE INTELLIGENCE ARTIFICIELLE (MIDJOURNEY®) – CRÉDIT: ROULARTA MEDIA GROUP

de comptes de l'utilisateur. En comparant deux empreintes, il est possible de vérifier plus efficacement l'identité.

«Imaginons le cas de Netflix, qui souhaite bloquer le partage d'un compte entre plusieurs personnes. En utilisant le *fingerprinting*, elle pourrait savoir si les informations de l'environnement numérique d'un abonné correspondent à ce qui est habituel. Si oui, elle en déduira que c'est bien lui, mais si la configuration présente des différences, elle pourra supposer que c'est une autre personne et suspendre la connexion», explicite Axel Legay.

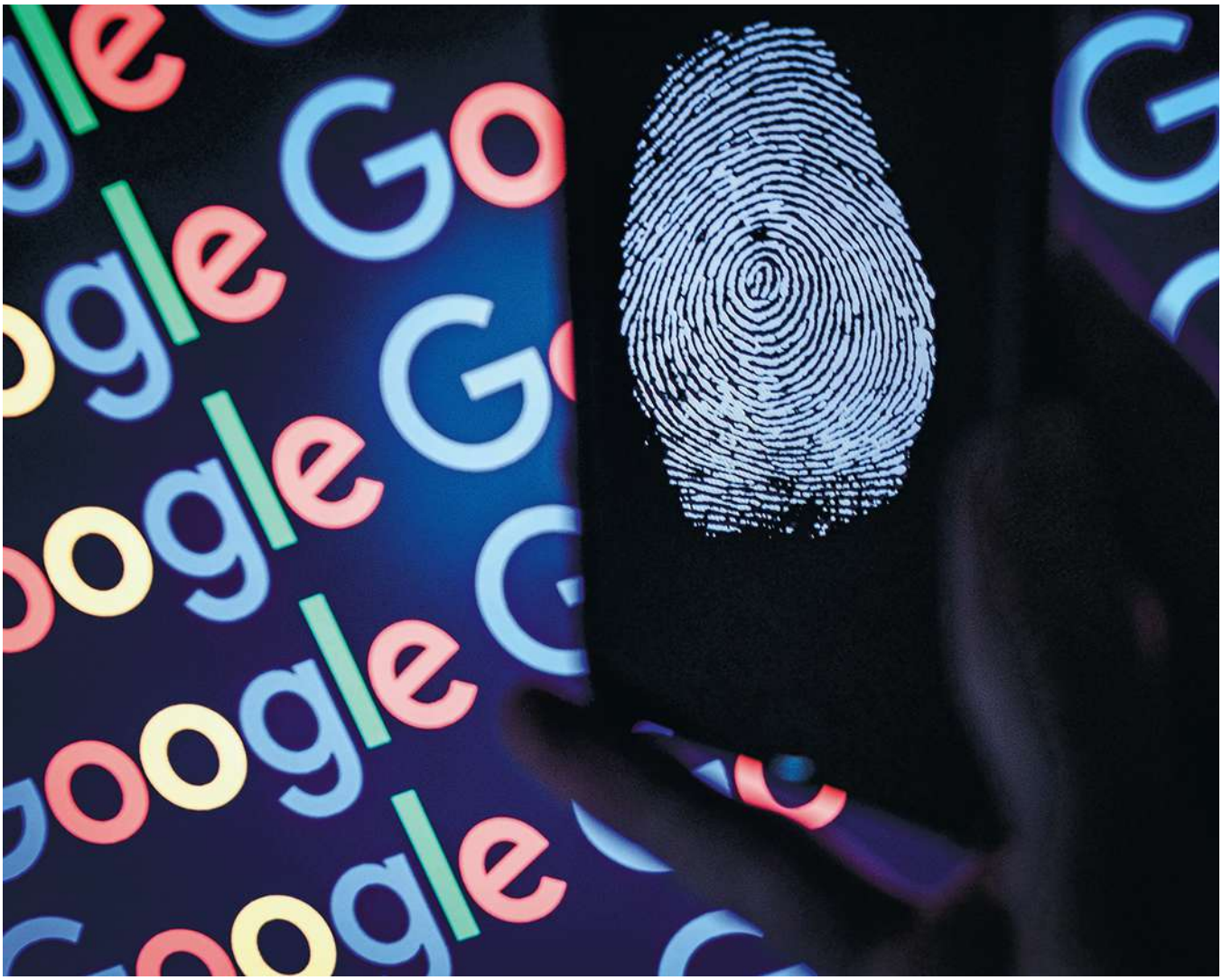
Google prendra les empreintes

Plus subtile, l'empreinte numérique n'a pas la même visibilité que le cookie, devenu contact obligatoire de l'internaute sur tous les sites Web lorsqu'il lui est demandé s'il souhaite les accepter ou les refuser. Plus discret par nature, le *fingerprinting* a toutefois vu un acteur de poids rappeler bruyamment son existence. Google autorise en effet cette technique dans l'exploitation de sa plateforme publicitaire depuis la mi-février.

En 2019, dans un message sur le blog de la société, le *fingerprinting* était pourtant décrié par le même Google, le jugeant «opaque» et «portant atteinte à la liberté de choix de l'utilisateur». La pression sur les revenus publicitaires, suivant le désamour envers les cookies, a visiblement poussé la firme de Mountain View à revoir sa position. Elle considère qu'il y a aujourd'hui suffisamment de garde-fous pour éviter les dérives.

Contactée par Le Vif à propos du *fingerprinting*, Google apporte des réponses formatées. Elle précise avoir mis à jour les règles de sa plateforme «pour tenir compte des nouvelles technologies de protection de la vie privée qui ...

«Nos partenaires devront continuer à être totalement transparents envers les utilisateurs sur les données qu'ils collectent et leur usage.»



GETTY

La pression sur les revenus publicitaires, et le désamour envers les cookies, a poussé Google à revoir sa position sur le *fingerprinting*.

… atténuent les risques et favorisent l'émergence de nouveaux canaux tels que la télévision connectée.»

Dans la documentation fournie, qui n'utilise jamais le terme *fingerprinting*, Google précise qu'elle sera moins directive avec ses partenaires, ceux-ci devant néanmoins «continuer à être totalement transparents envers les utilisateurs sur les données qu'ils collectent et leur usage». La société californienne précise qu'elle peut désormais «utiliser des protections axées sur la confidentialité qui aident les entreprises à atteindre leurs clients sur ces nouvelles plateformes sans avoir besoin de les réidentifier.»

«Les profits avant la vie privée»

Ces affirmations du géant technologique font bondir les militants pour un Web respectueux de la confidentialité. «En autorisant explicitement cette technologie, Google met en évidence la priorité qu'elle accorde aux profits par rapport à la protection de la vie privée. Les techniques de suivi que Google prétend essentielles pour la publicité en ligne exposent également les informations sensibles des individus aux courtiers en données (*data brokers*), aux sociétés de surveillance et aux forces de l'ordre», déplore Lena Cohen, de l'Electronic Frontier Foundation, citée par la BBC.

C'est également le point de vue d'Axel Legay. «Le but de Google n'est pas de voler vos données, mais de vendre des profils d'utilisateurs pour proposer un ciblage précis des audiences et valoriser sa publicité. Je suis plus tracassé par des hackers qui attaqueraient Google et voudraient piller les informations qu'elle détient. Celles-ci pourraient être détournées et exploitées à des fins malveillantes. Le risque est là, car les grandes sociétés de la tech sont parmi les plus attaquées.»

Ces questions de confidentialité des données sont malheureusement parfois délaissées par les utilisateurs, malgré les enjeux essentiels qu'elles représentent. «Les gens peuvent s'en désintéresser, soit parce qu'ils n'ont pas conscience des traces digitales qu'ils laissent, soit parce qu'ils ne s'en inquiètent pas. On peut légitimement estimer n'avoir rien à cacher, mais des informations sensibles, par exemple sur la santé, pourraient porter préjudice si elles étaient révélées ou utilisées à notre insu. Prendre conscience de sa possible identification, sur base de choses aussi simples que des paramètres dans un navigateur Internet, doit nous convaincre qu'il est difficile d'assurer son anonymat en ligne», détaille Julien Hendrickx, professeur d'ingénierie mathématique à l'UCLouvain.

Quid du RGPD?

La légalité de la technique interpelle également. Si les cookies sont désormais encadrés, l'empreinte numérique se trouve en zone grise. Aucun consentement n'est requis, le droit de refuser est techniquement difficile, la transparence sur l'utilisation des données est absente. Autant d'éléments que le RGPD avait pointés à l'encontre des cookies. «Le RGPD s'applique dès lors que des renseignements personnels sont concernés. La description des empreintes fait clairement référence à des données personnelles, puisqu'elles sont liées à un individu. On peut tout demander à un internaute, mais il doit être informé, donner son consentement éclairé et pouvoir accepter avec granularité ce qu'il transmet», détaille Fanny Coton, avocate spécialisée en droit de la vie privée au cabinet Lexing.

L'Autorité belge de protection des données abonde: «Le *fingerprinting* est considéré de la même manière que d'autres traceurs. Outre le RGPD, la directive ePrivacy s'applique également. Celle-ci précise que seuls les cookies (et autres traceurs) strictement nécessaires sont exemptés d'un consentement. Si traitement il y a, il faut le consentement valide de l'utilisateur.» Pas question donc d'échapper aux règles malgré le caractère purement technique des informations récoltées, même si elles peuvent sembler anodines prises séparément.

«Peut-on considérer que ce sont des données anonymes? Vaste question, reconnaît Axel Legay. Techniquement, un *hash (NDLR: une suite de caractères formant une empreinte numérique de manière cryptée)* est unique. Il est donc possible d'y voir une identification de l'utilisateur.» Parvenir à associer un *hash* à une personne ouvre la voie à un suivi beaucoup plus précis, avec un intérêt évident pour la publicité.

«Il faut encore rappeler que rien n'est gratuit dans le monde digital. Interdire les cookies partout et rendre la publicité plus compliquée, c'est mettre à mal l'accès gratuit à certains sites. La population doit se demander si elle accepte ce modèle d'échange de données contre des services gratuits, ou s'il est plus souhaitable de passer à un modèle payant», interroge l'expert.

Pas question d'échapper aux règles malgré le caractère purement technique des informations récoltées.

Comment y échapper?

La question de l'évitement du *fingerprinting* est technique et se répercute sur l'utilisabilité des sites Web. Connaître la langue de l'utilisateur ou la résolution d'un écran permet d'afficher correctement les informations. Cadenasser totalement toutes les caractéristiques transmises n'est pas souhaitable.

Certains navigateurs (Tor, Firefox, Brave et d'autres) proposent pourtant des modes de blocage d'empreinte numérique. L'une des pistes suivies est de maximiser la ressemblance entre utilisateurs: pour devenir anonyme au sein d'une foule, mieux vaut s'habiller comme tout le monde plutôt que de cacher son visage avec un masque. Installer séparément un bloqueur d'empreinte revient à mettre un masque, ajoutant finalement un paramètre différenciant, permettant de repérer une cible.

A l'inverse, le navigateur peut également tenter de rendre aléatoires plusieurs paramètres afin de «changer» virtuellement, de muer fréquemment. Si suffisamment de caractéristiques changent d'une fois à l'autre, il est plus complexe d'être identifié avec certitude.

La dernière solution consiste à bloquer les scripts permettant la prise d'empreinte numérique. Un ensemble de techniques à l'efficacité relative, toujours étudiées par les chercheurs en sécurité.

Plusieurs outils en ligne, comme amiunique.org, permettent de suivre les informations récoltées et la similitude, ou l'extrême singularité, de sa configuration. De quoi réaliser que sur le Net, l'anonymat reste compliqué et qu'aucun clic n'est véritablement gratuit. Vous reprendrez bien un cookie? ●